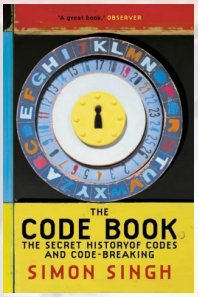

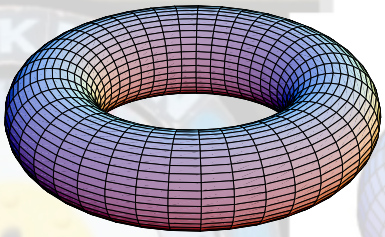

שיטות אריתמטיות בקריפטוגרפיה
המקום בו חזית המתמטיקה פוגשת את הביטקוין

ב- 2026 הצפנה אינה מוגבלת לשימושים צבאיים. היא בכל מקום סביבנו, מגנה על כל התקשורת האלקטרונית שלנו. מתמטיקה בכלל, ותורת המספרים בפרט, היא הבסיס לכמעט כל אלגוריתם הצפנה.

אנחנו נתמקד בתורה המתמטית שהיא בו זמנית המתקדמת ביותר - היתה למשל הבסיס להוכחת משפט פרמה, והמהווה את הבסיס לאלגוריתמי ההצפנה החדשניים והבטוחים ביותר כמו אלה שעליהם מבוסס הביטקוין: **תורת העקומים האליפטיים.**

בקורס תראו כמה מהמשפטים המפורסמים ביותר של המאה העשרים, כמו השערות Weil, וכיווני מחקר עכשויים, משמשים באלגוריתמים הקריפטוגרפיים הבטוחים ביותר היום. ואת המימוש שלהם בתוכנות מתקדמות המיועדות למחקר מתמטי Sage (המבוססת פייתון) ו- Julia.

חדש בקורס ב- 2026:

- שפת Julia
- הצפנה פוסט קוונטית באמצעות עקומים אליפטיים

מטרות הקורס:

- להציג את התורה של העקומים האליפטיים בגישה אלמנטרית. בתורת העקומים האליפטיים אפשר לנסח בקלות משפטים מתקדמים שלא נוכל להוכיח בכלים אלמנטריים אבל יוכלו לשמש בסיס לקורס מתקדם או קורס קריאה
- להציג שימושים של תורת מספרים ותורת העקומים האליפטיים להצפנה. בין היתר נראה איך מצפינים עם עקומים אליפטיים, איך מפרקים מספר גדול לגורמים ראשוניים ואיך מוכיחים שמספר הוא ראשוני. נראה כיצד משפטים קשים בתורת העקומים האליפטיים נחוצים על מנת ליצור שיטות הצפנה בטוחות
- להדגים כמה שיותר מהחומר הנלמד באמצעות מחשב. נראה את היכולת העכשוית להדגים ולגלות תוצאות חדשות באמצעות מחשבים (באמצעות חבילות תוכנה - **לא תידרש יכולת תכנות בקורס**)